DOCKET NO: 203223US-28

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF	:
SHINGO YAMAGUCHI	: EXAMINER: HA, LEYNNA A.
SERIAL NO: 09/863,384	:
FILED: MAY 24, 2001	: GROUP ART UNIT: 2135
FOR: METHOD AND SYSTEM FOR CONTROLLING ACCESS TO NETWORK RESOURCES BASED ON CONNECTION SECURITY	:

REPLY BRIEF

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

In response to the Examiner's Answer of August 9, 2007, Applicant submits the following comments in the present Reply Brief.

First, the Appeal Brief filed April 18, 2007 is believed to clearly set forth Applicant's position as to how the pending claims distinguish over the applied art. The present Reply Brief addresses additional comments newly presented in the "Response to Argument" section beginning at page 13 on the Examiner's Answer.

By way of background, the present invention is directed to a system that can allow different computing devices to connect to a network, and a level of access on the network is based on whether the computing devices connect to the network in an encrypted or non-encrypted manner. With reference to Figure 2A in the present specification as a non-limiting example, if either of the computing devices 2, 6 connects to the intermediate device 10 through an encrypted connection, a firewall setting for level 1 access is provided, and in that

case a high level of access to various network resources, including a file server, can be provided. Alternatively, if no encryption is utilized for the connection between either of the computing devices 2, 6 and the intermediate device 10, a firewall setting for level 2 access is utilized, and at that point the user of the computing devices 2, 6 may only have limited access to resources on the network, including access to the Internet and an email server.

The outstanding rejection recognizes that U.S. patent 6,732,176 to Stewart does not discuss connecting to a computer network via an encrypted or non-encrypted connection, and wherein a first level of the security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted.[1] To overcome the recognized deficiencies in Stewart the outstanding rejection cites U.S. patent 6,453,159 to Lewis.

Simply stated, for the combination of teachings to meet the claim limitations Lewis would have to suggest to one of ordinary skill in the art modifying Stewart determine whether the wireless access points 120 were connecting to the network 130 via an encrypted or non-encrypted connection, and then control access to different network resources based on that determined connection.

Lewis, however, does not disclose or suggest changing the access level to network resources based on whether a connection to a network is encrypted or non-encrypted, and thus one of ordinary skill in the art clearly would not have taken such teachings from Lewis and would not have modified Stewart in a way to meet the claim limitations.

In contrast to the claimed features, Lewis indicates that if the system therein receives a non-encrypted message from an access point 54, and if it is determined that the access point

[1] Examiner's Answer of August 9, 2007, page 5, first full paragraph, as one example.

54 is included in a table indicating that access point 54 is authorized, the access point 54 may be permitted to communicate in a non-secure manner.[2]

Lewis does not, however, disclose or suggest that a level of access to network resources is changed based on whether the access point 54 communicates in an encrypted or non-encrypted format. Appellant also points out the Examiner's Answer does not indicate where Lewis discloses or suggests such features.

In the "Response to Argument" section, in the paragraph bridging pages 13 and 14, the Examiner's Answer points out how Stewart discloses controlling a level of access on a network.

In reply, Appellant notes such disclosures in Stewart are irrelevant to the claims. The claims are not merely directed to controlling a level of access to resources on a network, but to specifically controlling that level of access based on whether a computing device is connecting to the network based on an encrypted or non-encrypted format. Controlling a level of access on a network as in Stewart is unrelated to that claim feature of ***how the level of access is set***. Stewart clearly does not disclose or suggest the claim features in that respect, and the comments in the paragraph bridging pages 13 and 14 in the Examiner's Answer are irrelevant to those claim features.

The Examiner's Answer, at the paragraph bridging pages 14 and 15, further notes how Lewis can allow both encrypted and non-encrypted communication with the network. Such features, however, are also irrelevant to the claims. The claims do not broadly indicate allowing both encrypted and non-encrypted access to a network. Instead, the claims indicate a determination of whether a connection is encrypted or non-encrypted controls a level of access to resources on the network. Lewis does not disclose or suggest such features, and the Examiner's Answer does not point to any disclosures in Lewis to disclose or suggest such

[2] Lewis at column 13, lines 17-25.

features. Absent such a disclosure in Lewis no combination of teachings of Lewis in view of Stewart would fully meet the claim limitations.

The paragraph bridging pages 15 and 16 in the Examiner's Answer points to disclosures in Lewis directed to utilizing a table that can indicate devices authorized to communicate with a network in either encrypted or non-encrypted format.

Again, however, such disclosures in Lewis are irrelevant to the claims.

The paragraph bridging pages 15 and 16 in the Examiner's Answer also states incorrectly that "[t]he claimed determining the level of security does not include a method or device to carry out the process".

In reply Applicant notes the claims positively recite a level of security of the computer network connection is determined "based on whether the computer network connection to connect the computing device to the intermediate device is encrypted". Thereby, the claims clearly recite how the level of security is set, namely on a determination of whether a connection is encrypted or not. The Examiner's Answer has not indicated how such a feature is met by either Stewart or Lewis, and as discussed in the Appeal Brief in detail such a feature is believed to clearly distinguish over both Stewart and Lewis.

The paragraph bridging pages 16 and 17 in the Examiner's Answer appears to indicate how the combination of teachings of Stewart in view of Lewis fully meets the claim limitations. However, those statements do not appear to address the above-noted comments that neither Stewart nor Lewis discloses or suggests setting a level of access to network resources based on determining whether a connection to the network is encrypted or non-encrypted.

Stated another way, Stewart discloses allowing different access levels to network resources. Lewis discloses allowing non-encrypted access to a network if a device is preregistered as authorized to communicate in a non-encrypted manner. If the teachings of

Stewart and Lewis were combined, that would suggest to one of ordinary skill in the art a system that allows different access levels to network resources, and that allows non-encrypted devices to communicate with the network if previously authorized. Such a combination of teachings would ***not*** have suggested to one of ordinary skill in the art to change the level of access of the network resources based on whether a connection to the network was encrypted or non-encrypted. Neither Stewart nor Lewis disclose or suggest such features, and no combination of Stewart and Lewis would disclose or suggest such features.

For these foregoing reasons, and the reasons provided in the Appeal Brief filed April 18, 2007, Appellant submits the outstanding rejection based on Stewart in view of Lewis must be REVERSED.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

James J. Kulbaski
Attorney of Record
Registration No. 34,648

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 03/06)

I:\ATTY\SNS\20's\203223\203223US-RB.DOC